IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MICHAEL RENNINGER, SR., individually and on behalf of all others similarly situated, Plaintiff, v. ANTHEM, INC., an Indiana Corporation, Defendant.	CASE NO.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

NOW COMES Plaintiff Michael Renninger, Sr., by and through his undersigned counsel, individually and on behalf of all others similarly situated, and hereby files this Class Action Complaint against Anthem, Inc. ("Defendant" or "Anthem"). In support thereof, Plaintiff states and alleges as follows:

NATURE OF THE ACTION

1. Defendant comprises the second largest health insurer in the United States, providing health care coverage to approximately 37.5 million people. In 2014 alone Defendant claimed net income totaling approximately $2.6 billion.

2. On February 4, 2015, Anthem confirmed that the personal health, identification, and financial information of millions of Anthem customers was improperly accessed and taken from the IT systems of Anthem (the "Data Breach") and, furthermore, that the Data Breach extended into all of Anthem's business units.[1] On a newly created website, Anthem then announced that the Data Breach affected all lines of Anthem business, including multiple brands

[1] Joseph R. Swedish, *From the Desk of Joseph R. Swedish*, www.anthemfacts.com (hereinafter "Anthem CEO Letter"). Unless otherwise noted, all websites cited herein were last visited on Feb. 26, 2015.

Anthem uses to market its healthcare plans, including Anthem Blue Cross, Anthem BlueCross BlueShield, BlueCross BlueShield of Georgia, Empire BlueCross and BlueShield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare.[2]

3. Anthem also announced that the Data Breach affected BlueCross BlueShield plans not owned by Anthem, via compromise of BlueCard membership cards. The Blue Cross Blue Shield Association's BlueCard is a national program that enables members of one Blue Cross Blue Shield Plan to obtain healthcare services while traveling or living in another Blue Cross Blue Shield service area. "The program links participating healthcare providers with the independent Blue Cross and Blue Shield Plans across the country and in more than 200 countries and territories worldwide through a single electronic network for claims processing and reimbursement."[3]

4. Plaintiff brings this Class Action Complaint on behalf of himself and all other persons whose personal health, identification, and financial information was improperly obtained during the Data Breach.

5. As a result of Anthem's failure to protect extremely confidential data, the personal health, identification, and financial information of Plaintiff and the members of the Class (including former customers and employees of Anthem) has been taken, including full legal names, birth dates, Social Security numbers, medical identification numbers, health histories, street addresses, email addresses, employment information, income data, and other personal information. The Data Breach affects at least tens of millions of records as a result of

---

[2] Anthem, *Frequently Asked Questions*, www.anthemfacts.com/faq (hereinafter "Anthem FAQ").

[3] *Id.*

the compromise of a database containing personal information for 80 million Anthem customers and employees.

6. Anthem had a duty to protect the private, highly sensitive, confidential personal health, identification, and financial information of Plaintiff and members of the Class.

7. Anthem failed to safeguard and prevent vulnerabilities from being taken advantage of in its computer and information technology systems.

8. Plaintiff and the proposed Class members have a possessory interest in their personal health, identification, and financial information and an interest in it remaining private because that information, including incredibly private and sensitive information such as Social Security numbers and patient identification numbers, accompanied by birth dates and addresses, has substantial value not only to Plaintiff and the proposed Class members, but also to criminals who traffic in such information, using it to steal the identities of victims like Plaintiff and the Class.

9. Because of the real threat of immediate harm, as well as the intrinsic value of the stolen information itself, Plaintiff and the proposed Class members have suffered an immediate and present injury to their privacy and possessory interest as a direct result of Defendant's negligent failure to safeguard Plaintiff's and the proposed Class members' personal health, identification and financial information, as well as the breach of its agreement to do the same.

10. Moreover, Plaintiff and the proposed Class members have been or are at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse, and have been forced to spend considerable time and money to protect themselves—and face years of constant surveillance of their financial and medical records—monitoring, loss of rights, and

potential medical problems, among other harms - as a result of Anthem's conduct in failing to adequately protect their personal health, identification and financial information.

THE PARTIES

11. Plaintiff, Michael Renninger, Sr., is an adult individual residing in Pennsylvania. Plaintiff is a citizen of the State of Pennsylvania. Plaintiff's personal health, identification, and financial information were compromised in the Data Breach.

12. Defendant Anthem Inc., known as WellPoint, Inc. until December 2014, is an Indiana corporation headquartered in Indianapolis, Indiana and registered to do business in Missouri.

13. Anthem Inc. is headquartered at 120 Monument Circle, Indianapolis, Indiana, 46204.

14. Anthem reported $71 billion in total revenues and $59.5 billion in total assets in fiscal year 2013.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because: (i) the Class (as defined below) has more than 100 Class members; (ii) the amount at issue exceeds five million dollars, exclusive of interest and costs; and (iii) minimal diversity exists as Plaintiff and Defendant are citizens of different states.

16. This Court has personal jurisdiction over Anthem because Anthem is authorized to do and does do business in the State of Pennsylvania.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because many of the acts and transactions giving rise to this action occurred in this District and because Anthem is subject to personal jurisdiction in this District.

FACTUAL BACKGROUND AND ALLEGATIONS

I. ANTHEM'S COLLECTION OF PERSONAL, CONFIDENTAL INFORMATION

18. Anthem is the largest for-profit managed health care company in the Blue Cross and Blue Shield Association, and the second largest health insurer in the United States. Anthem operates plans including Anthem Blue Cross (coverage in California), Anthem Blue Cross Blue Shield (coverage in Colorado, Connecticut, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, Ohio, Virginia, and Wisconsin), BlueCross BlueShield of Georgia (coverage in Georgia), Empire BlueCross and BlueShield (coverage in New York), Amerigroup (coverage for state and federally sponsored beneficiaries and federal employees in 26 states), Caremore (coverage in California, Nevada, and Arizona), Unicare (nationwide Medicare coverage and former coverage in Illinois and Texas), Healthlink (coverage in the Midwest), and DeCare (nationwide dental coverage). Anthem provides coverage for 37.5 million Americans.

19. Anthem also participates in the BlueCard program, which is national program of the Blue Cross Blue Shield Association that enables members of one BlueCross BlueShield plan to obtain healthcare services while traveling or living in another BlueCross BlueShield service area.

20. Plaintiff and members of the proposed Class have, or previously had, health insurance issued by Anthem or another member of the BlueCard program. Anthem has either required them to provide their personal health, identification and financial information, including full legal names, dates of birth, Social Security numbers, billing information, street addresses, email addresses, employment information, income data, and highly confidential personal health history and other information to become an insured under Anthem's insurance coverage or has

obtained that information from other Blue Cross/Blue Shield entities under the BlueCard program in order to provide health care coverage for non-Anthem insureds.

21. Anthem was, and currently is well aware that the sensitive personal information provided to them by Class members is confidential, highly sensitive, and vulnerable to attack.

22. Plaintiff and the proposed Class members and Defendant agreed that, as part of the health care services provided to Plaintiff and the proposed Class Members, Defendant would protect the patient identification data of Plaintiff and the proposed Class members.

23. At all times during and after the collection of the highly sensitive data described in paragraph 20, Anthem promised Plaintiff and the members of the Class that it "maintain[] policies that protect the confidentiality of personal information,[4] including Social Security Numbers, obtained from their members and associates in the course of their regular business functions" and that they are "committed to protecting information about [their] customers and associates, especially the confidential nature of their personal information."[5]

24. Indeed, Anthem has claimed and currently claims that it has numerous procedures in place to protect the sensitive and personal information of its insured, including:

> Anthem Blue Cross and Blue Shield's Privacy Policy imposes a number of standards to (1) guard the confidentiality of Social Security numbers and other personal information, (2) prohibit the unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers;

---

[4] Anthem describes personal information as follows: "Personal Information is information that is capable of being associated with an individual through one or more identifiers including but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." *See* Privacy, ANTHEM, https://www.anthem.com/health-insurance/about-us/privacy.

[5] *Id.*

> Anthem Blue Cross and Blue Shield will not use or share Social Security numbers or personal information with anyone outside the company except when permitted or required by federal and state law;
>
> Anthem Blue Cross and Blue Shield Associates must only access Social Security numbers or personal information as required by their job duties. Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law; and
>
> Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.[6]

25. Defendant published a code of conduct, called "HONcode."[7] In it, Defendant states that "Health on the Net Foundation is available to verify and improve the quality of health information on the Net. Anthem decided to request Health on the Net Foundation for a membership [sic] so that you know our health content complies with the eight principles of the HONcode."

26. HONcode includes a principle of "Privacy," which provides, in relevant part, as follows: "Confidentiality of data relating to individual patients and visitors to a medical/health Web site, including their identity, is respected by this Web site. The Web site owners undertake to honour or exceed the legal requirements of medical/health information privacy that apply in the country and state where the Web site and mirror sites are located."[8]

27. Further, in Anthem's Code of Conduct for its Suppliers, Defendant provides that:

> ***Anthem, Inc. and its workforce have a responsibility to protect the confidentiality of the Protected Health Information (PHI) it collects uses and discloses about its members and applicants***. Suppliers that provide a service to or on behalf of Anthem which requires the use or disclosure of PHI shall be deemed Business Associates, in accordance with the Health

---

6 *Id.*

7 HONcode, ANTHEM, https://www.anthem.com/health-insurance/about-us/honcode.

8 *See* http://www.hon.ch/HONcode/Conduct.html.

> Insurance Portability and Accountability Act of 1996, and shall enter into a Business Associate Agreement and Security Addendum with Anthem.[9]

28. As described below, Anthem failed to follow these policies and also failed to take reasonable steps or put in place adequate protections to safeguard the personal health, identification, and financial information of Plaintiff and the proposed Class Members.

II. THE BREACH AND ANTHEM'S SECURITY PRACTICES

29. The personal health, identification, and financial information of Plaintiff and the proposed Class members, while under the control of Defendant, was accessed without Plaintiff or proposed Class members' authorization. The exact details regarding the mechanics of the Data Breach are mostly unknown and will be further determined during discovery.

30. On February 4, 2015, Anthem announced that its information technology systems had been hacked, resulting in the improper disclosure of personal health, identification, and financial information of both current and former customers and employees. The *Wall Street Journal* estimates that 80 million people may have had their data accessed without authorization.[10] The Data Breach included the loss of "personal information relating to consumers and Anthem Blue Cross employees who are currently covered, or who have received coverage in the past."[11]

---

[9] *See* Company Policies and Procedures at 5 (Oct. 17, 2014) (emphasis added), *available at* http://www.antheminc.com/prodcontrib/groups/wellpoint/@wp_suppliers/documents/wlp_assets/pw_e226861.pdf.

[10] Anna Wilde Mathews & Danny Yadron, *Anthem Health Insurer Hit by Big Data Breach*, WALL STREET JOURNAL (Feb. 5, 2015) at A1, *available at* http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720.

[11] Chad Terhune, *Anthem Hack Exposes Data on 80 Million; Experts Warn of Identity Theft*, L.A. TIMES, http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1.

31. The personal health, identification, and financial information of Plaintiff and the members of the Class, including, but not necessarily limited to, full legal names, birth dates, Social Security numbers, medical identification numbers, health histories, street addresses, email addresses, employment information, income data, and other personal information was improperly accessed and collected without the authorization of Plaintiff and the members of the Class while that information was in the custody and control of Anthem.

32. Anthem has publicly stated that it discovered the Data Breach between January 27, 2015, and January 29, 2015, and then announced it on February 4, 2015. That assertion is contradicted, however, by a memo sent by Anthem to its clients, which notes that the unauthorized activity on their information technology platforms dates back to at least December 10, 2014, meaning that Anthem's customer database was accessed for more than a month before detection of any kind.[12] More recent reports suggest the Data Breach could date back to April of 2014.[13]

33. The Data Breach was made possible as a result of Anthem's lax security policies. By way of illustration and without limitation, on information and belief, Anthem failed to (1) require multi-factor authentication, (2) properly encrypt data, (3) establish adequate firewalls to handle a server intrusion contingency, (4) address security vulnerabilities to adequately protect the confidential information contained in its computer network, and (5) employ monitoring technology that was sufficiently sensitive to detect unusual flows of data out of its computer systems.

---

[12] Brian Krebs, *China to Blame in Anthem Hack?*, KREBS ON SECURITY, http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/#more-29778.

[13] Brian Krebs, *Anthem Breach May Have Started In April 2014*, KREBS ON SECURITY, http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

34. For example, upon information and belief, hackers gained access to Anthem's internal systems using stolen credentials, i.e., the username and password, of one of the company's senior administrators.[14] In total, the credentials of five of Anthem's tech employees were compromised in the Anthem breach.[15]

35. These usernames and passwords gave hackers access to the breadth of Anthem's internal systems, as well as the personal and confidential information of Plaintiff and the Class because Anthem failed to employ multi-factor authentication[16] in protecting its internal systems.[17]

36. When multi-factor authentication is used, there are multiple layers of protection. The first layer of protection involves a username and password. After the username and password are entered, the second layer of protection is enacted. For example, after a correct username and password are entered, the secondary authentication system will send a lengthy number to the users' personal device, such as a cellphone, and that number must be then be immediately entered to complete the login process. Without access to this second layer of authentication, someone possessing only the username and password is denied access.

37. Because Anthem failed to use this basic protection (which has been widely available for more than a decade) and instead employed single factor authentication, i.e., a single

---

[14] Scott Rea, *Anthem Hack: Was It Preventable?*, DIGICERT https://blog.digicert.com/anthem-hack-preventable/.

[15] Steve Ragan, *Anthem: How Does A Breach Like This Happen*, CSO, http://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html?page=2.

[16] Multi-factor authentication consists of using a personal device, such as a card, key fab, token, or smart phone app, to verify the identity of an administrator or other technical employee.

[17] Sean Michael Kerner, *Anthem Data Breach Exposed 80 Million Users to Risk*, eWeek, http://www.eweek.com/security/anthem-data-breach-exposed-80-million-users-to-risk.html; J.K. Wall, *Anthem's IT System Had Cracks Before Hack*, IBJ (Feb. 14, 2014) http://www.ibj.com/articles/51789-anthems-it-system-had-cracks-before-hack.

user name and password, hackers were able to access Anthem's systems after they gained the credentials of their tech employees.[18] Multi-factor authentication would have prevented this because the hackers would have had to gain access to the employees' personal device in order for the usernames and passwords to work. Use of multi-factor authentication is standard and best practice for any area in which there is sensitive data.[19]

38. Indeed, after the attack, Anthem shut down all IT areas that did not require or use multi-factor authentication and, as of Feb. 8, "reworked all its IT accounts that [had] privileged access to sensitive information to [] require three layers of authentication—a permanent login, a physical token, and a temporary password that changes every few hours."[20]

39. Another example of Anthem's failed security policies is Anthem's failure to encrypt its databases containing the personal information of Plaintiff and members of the Class.[21]

40. Anthem's failure to encrypt personal health, identification, and financial information in its information technology systems is conduct that is roundly criticized by security experts. As Trent Telford, chief executive of Covata, a data security firm in Reston, Virginia, noted, "'It is irresponsible for businesses not to encrypt the data . . . . We have to assume the thieves are either in the house or are going to break in. They will always build a taller ladder to climb over your perimeter security.'"[22] But Anthem has been slow in adopting

---

18 Rea, *supra* note 14.

19 Wall, *supra* note 17.

20 *Id.*

21 Terhune, *supra* note 11.

22 *Id.*

measures like keeping personal information in separate databases that can be closed off in an attack and is less secure than other companies that store the same types of customer data.[23]

41. Anthem's failure to encrypt Social Security numbers, along with other personal health, identification and financial information, is especially egregious, because "Social Security numbers are a particularly popular target for hackers. Combinations of Social Security numbers, birth dates and names sell for more than even credit card numbers in an increasingly sophisticated black market, where such information is sold and resold through popular auction sites."[24] The reason for the increased value of this data is simple – a credit card number can be cancelled or changed in minutes, while Social Security numbers, birth dates, etc. are largely permanent identifiers that, once disclosed, cannot be easily changed to prevent fraud.

42. A third example of Anthem's security failures is the absence of behavioral analytics technologies "that could have raised a flag immediately when [] patient records were transferred."[25]

43. Instead of using this up-to-date, advanced technology, Anthem employed a data loss prevention technology that monitored data traffic on its network. J.J. Thompson, CEO of Indianapolis-based IT security firm Rook Security, has stated that "[t]here's a known weakness in that technology."[26] He added that use of behavioral analytics technology is superior because it

---

23 Reed Abelson & Matthew Goldstein, *Anthem Hacking Points to Security Vulnerability of Health Care Industry*, N.Y. TIMES, http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html.

24 Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES, http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html.

25 Wall, *supra* note 17.

26 *Id.*

"identif[ies] a pattern of normal behavior and then receive a notice when abnormal behavior takes place."[27]

44. In any event, Fred Cate, an IT expert at Indiana University, stated that Anthem's systems still should have detected the transfer of consumer data internally and "the fact that it took seven weeks is going to require some explanation. To not notice that is pretty shocking."[28]

III. ANTHEM'S CONDUCT VIOLATED INDUSTRY STANDARDS AND OTHER APPLICABLE STATUTES AND GUIDELINES

45. The 2013 Identity Fraud Report released by Javelin Strategy & Research reports that in 2012 identity fraud incidents increased by more than one million victims, and fraudsters stole nearly $21 billion in actual theft. The study found 12.6 million victims of identity fraud in the United States in the past year, which equates to 1 victim every 3 seconds. The report also found that nearly 1 in 4 data breach letter recipients became a victim of identity theft, with breaches involving Social Security numbers to be the most damaging: consumers who had their Social Security number compromised in a data breach were 5 times more likely to be a victim than an average consumer.

46. Given the well-publicized increases in data thefts, Defendant had a duty to protect the private, highly sensitive, confidential personal health, identification, and financial information of Plaintiff and the proposed Class members.

47. Indeed, Defendant was statutorily obligated to adequately protect the information in question because the personal health, identification, and financial information that was copied and transferred from Defendant's computer systems is considered protected information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 29 U.S.C.A. §§

---

27 *Id.*

28 *Id.*

1181 *et seq.*, because it includes patient names, addresses, birthdates, telephone numbers and Social Security numbers.

48. HIPAA required Defendant to "reasonably protect" the copied data from "any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(1)(2)(i). Federal regulations also required Defendant to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." *Id.* at § 164.530(c)(1).

49. Defendant violated HIPAA by failing to maintain the confidentiality of Plaintiff's and the proposed Class members' protected personal health, identification and financial information.

50. In addition to failing to comply with basic rules of conduct and HIPAA, Defendant failed to employ reasonable and industry standard safeguards and procedures that would have prevented vulnerabilities in its information technology systems from being exploited by hackers.

51. To assist companies in protecting the security of sensitive personal and financial information, the Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" (the "FTC Report"). In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft.

52. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a) Keep inventory of all computers and laptops where the company stores sensitive data;

b) Do not collect personal information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c) Use Social Security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d) Encrypt the personal information, particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

e) Do not store sensitive computer data on any computer with an Internet connection or access unless it is essential for conducting the business;

f) Control access to sensitive information by requiring that employees use "strong" passwords; and

g) Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to personally identifying information.

53. Defendant failed to employ these and other basic safeguards and, as a result of that failure, unauthorized third parties were able to bypass Defendant's inadequate security measures and successfully copy and transfer personal health, identification, and financial information of Plaintiff and the proposed Class members and by failing to dispose of Plaintiff's and the members of the Class's personal health, identification, and financial information in a reasonable and appropriate manner.

54. Anthem's failure to encrypt sensitive personal health, identification, and financial information violates current federal privacy regulations and industry standards. These standards are particularly important for health insurance companies, which are encouraged to share medical records between doctors, hospitals, and insurers by the federal government, and thus must be extra careful in ensuring that the databases used to store such information are secure.[29]

[29] *See* Abelson & Goldstein, *supra* note 23.

55. Anthem's failure to adequately protect personal health, identification, and financial information of its current and past customers, current and past potential customers, and current and past employees, including Plaintiff and members of the Class, is consistent with its prior history of security weaknesses and failures to maintain adequate safeguards of online data. In 2013, Anthem paid $1.7 million to resolve federal allegations with the U.S. Department of Health and Human Services that it exposed protected health information of over six hundred thousand people online because of security weaknesses and "inadequate safeguards in an online application database and left names, birth dates, Social Security numbers and health data accessible to unauthorized people."[30] That investigation found that Anthem "didn't adequately implement policies for authorizing access to the database and didn't have technical safeguards in place to verify users."[31]

56. As described above, Defendant violated federal guidelines and failed to meet current data security industry standards by failing to ensure adequate security over Plaintiff's and the proposed Class members' personal health, identification, and financial information and by failing to retain Plaintiff's and the proposed Class members' personal health, identification, and financial information in a secure and safe manner.

57. Anthem's failure to follow its own internal policies, as well as its failure to follow both basic and best data security practices has caused myriad harm to Plaintiff and the Class.

---

30 Terhune, *supra* note 11.

31 *Id.*

IV. THE CLASS WAS DAMAGED BY ANTHEM'S CONDUCT AND/OR INACTION

58. The damage to the Class in this case is particularly egregious as compared to other data breaches involving consumers. As Kate Cox reported in the Consumerist, "Any data breach is bad, but the more personal they are – and the more widespread – the worse. And by both metrics, the hack just announced by major health insurer Anthem is particularly terrible."[32] This is both because the "data breach extended across all of Anthem's business[es], possibly affecting customers at large employers, individual policyholders and people enrolled in Medicaid managed-care plans" and because "the wide array of personal information taken opens up more possibilities for mischief."[33]

59. Anthem's failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiff's and the members of the Class's personal health, identification, and financial information has also put members of the Class at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse. As Paul Stephens, Director of Policy and Advocacy at the Privacy Rights Clearinghouse in San Diego, said, the wide array of types of personal information opens up more possibilities for intrusions and indicates that another attack is imminent: "'You essentially have the keys to the kingdom to commit any type of identity theft . . . . The information can be used not only to establish new credit accounts but also potentially penetrate existing accounts at financial institutions or a stock brokerage. The scope of the information involved is incredible.'"[34]

60. Significantly, Anthem's offer to provide free credit monitoring to impacted Class

---

32 Kate Cox, *'Tens of Millions' of Personal Records Stolen in Attack on Health Insurance Company Anthem*, CONSUMERIST, http://consumerist.com/2015/02/05/tens-of-millions-of-personal-records-stolen-in-hack-on-health-insurance-company-anthem/.

33 Terhune, *supra* note 11.

34 *Id.*

members will not stop medical identity theft as a result of the Data Breach. Because the Data Breach involved compromise of medical identification, numbers on customer health insurance cards, and other personal information, "[c]riminals can use those numbers at hospitals, emergency rooms and pharmacies to receive care and prescriptions, racking up charges and wrecking victims' medical records." As Bob Gregg, CEO of ID Experts explained, "[i]t's like an unlimited credit card that gets you 'free' access to expensive services and drugs . . . . Everyone thinks about credit cards and bank accounts, but medical identity theft can be much more damaging and extremely hard to fix." Any medical care received using fraudulent medical identification gets added to the health records attached to the identification number, and may take months or years to surface.[35]

61. Accordingly, Anthem's failure to protect personal health, identification, and financial information may also have medical implications for Class members for years to come. As NBC News reported, "[i]magine an unwitting medical ID theft victim who is rushed to the hospital for emergency gallbladder removal, but the patient's record shows the gallbladder was removed last year. That could cause confusion for the healthcare providers and serious delays in treatment, as could incorrect information about blood types or possible drug interactions."[36]

62. Moreover, although Anthem admits the importance of monitoring the credit of the class going forward, it will not reimburse the Class for any immediate action taken by any member. Anthem's own website includes the following in the FAQ section:

If I choose to purchase credit monitoring and repair services effective immediately, will Anthem reimburse me?

---

35 Julianne Pepitone, *Anthem Hack: Credit Monitoring Won't Catch Medical Identity Theft*, NBC NEWS (Feb. 5, 2015), http://www.nbcnews.com/tech/security/anthem-hack-credit-monitoring-wont-catch-medical-identity-theft-n300836.

36 *Id.*

> No. Anthem is contracting with a trusted vendor to provide free identity repair services, which will be retroactive to the date of the potential exposure, and credit monitoring to all those impacted, and will not reimburse for services that you may have independently purchased.[37]

63. As such, the Class will either incur additional expenses that will not be reimbursed by Defendant and/or additional exposure and risk until Anthem chooses the contractor and provides the monitoring to the Class.

64. In addition to the ongoing and continued damage to the Class as a result of their increased and continued exposure to identity and medical theft as a result of the Data Breach, Class members have been harmed in that they paid for protections and services they did not receive when being provided healthcare by Defendant. A portion of the consideration paid for healthcare by Plaintiff and the proposed Class members was accepted by Defendant and was allocated to protecting and securing Plaintiff's and the proposed Class members' personal health, identification, and financial information and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and consumers, such as Plaintiff and the proposed Class members, added value to the health care services provided by agreeing to protect their protected personal health, identification and financial information.

65. Because of the real threat of immediate harm, the intrinsic value of the stolen information itself and the failure of Defendant to provide Plaintiff and the proposed Class with the benefit of the bargain made when obtaining healthcare from Anthem, Plaintiff and members of the Class have suffered an immediate and present financial injury as well as an injury to their privacy and possessory interests in their sensitive personal information. All of these damages

[37] Anthem FAQ, https://www.anthemfacts.com/faq.

flow directly from Defendant's negligent failure to safeguard this sensitive information as well as the breach of its agreement to do the same.

66. Moreover, Plaintiff and the proposed Class members have been or are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse, and have been forced to spend considerable time and money to protect themselves – and face years of constant surveillance of their financial and medical records, monitoring, loss of rights, and potential medical problems, among other harms – as a result of Anthem's conduct in failing to adequately protect their personal health, identification and financial information.

67. In addition to these losses, Plaintiff and the Class were also harmed by Defendant's inexcusable failure to provide timely notification to Plaintiff and proposed Class members of the Data Breach. That failure deprived Plaintiff and proposed Class members of critical time to protect themselves from, among other injuries, identity theft.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this action on his own behalf and on behalf all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

69. The Class is defined as follows:

> All persons whose personal health, identification, and financial information was contained in or on the Anthem computer system and whose personal health, identification, or financial information was stolen or otherwise misappropriated as a result of the Data Breach that was announced on or about February 4, 2015 (collectively, the "Class").
>
> Excluded from the Class are Defendant; officers and directors of Defendant; any entity in which Defendant has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendant, and; the Court and its officers, employees, and relatives.

70. Plaintiff is a member of the Class he seeks to represent.

71. This action satisfies the procedural requirements set forth in Rule 23 of the Federal Rules of Civil Procedure.

72. The conduct of Defendant has caused injury to members of the Class.

73. The Class is so numerous that joinder of all members is impracticable, as approximately 80 million individuals' personal health, identification or financial information may have been compromised.

74. The members of the Class are readily ascertainable, as they can be identified by records maintained by Defendant. Notice can be provided by means permissible under the Federal Rules of Civil Procedure.

75. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Anthem failed to provide adequate security and or protection for its computer systems containing Plaintiff's and members of the potential Class's personal health, identification or financial information;

b. Whether Anthem's conduct resulted in the unauthorized breach of its computer systems containing Plaintiff's and members of the potential Class's personal health, identification or financial information;

c. Whether Anthem improperly retained Plaintiff's and members of the potential Class's personal health, identification or financial information;

d. Whether Anthem disclosed (or directly or indirectly caused to be disclosed) private personal health, identification or financial information of Plaintiff and members of the potential Class;

e. Whether Anthem owed a legal duty to Plaintiff and members of the potential Class to use reasonable care in connection with its use and retention of personal health, identification or financial information;

f. Whether Anthem breached its duties to exercise reasonable due care in obtaining, using, retaining, and safeguarding Plaintiff's and members of the potential Class's personal health, identification or financial information;

g. Whether Anthem was negligent;

h. Whether Anthem's breach of its duties proximately caused damages to Plaintiff and the other members of the Class;

i. Whether Anthem is in breach of contract;

j. Whether Anthem violated Indiana Code §§ 24-5-0.5, *et seq*. and other relevant consumer protection statutes;

k. Whether Plaintiff and members of the Class have suffered damages, including but not limited to, an increased risk of identity theft as a result of Anthem's failure to protect Plaintiff's and the Class members' personal health, identification or financial information; and

l. Whether Plaintiff and other members of the Class are entitled to compensation, damages, and/or other relief as a result of the breach of duties alleged herein.

76. Plaintiff's claims are typical of the claims of all members of the Class. The same events and conduct that give rise to Plaintiff's claims and legal theories also give rise to the claims and legal theories of the Class. Specifically, Plaintiff's and members of the Class's claims arise from Anthem's failure to install and maintain reasonable security measures to

protect Plaintiff's and members of the Class's personal health, identification and financial information.

77. The conduct of Anthem has caused injury and/or imminent threat of injury to Plaintiff and members of the Class.

78. Plaintiff is a member of the putative Class, possesses the same interests, and suffered the same injuries as Class members, making her interests coextensive with those of the Class. The interests of Plaintiff and the Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

79. Anthem has acted and refused to act on grounds generally applicable to the Class described herein.

80. Prosecuting separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Anthem.

81. Plaintiff will fairly and adequately represent the interests of the Class. There are no disabling conflicts of interest between Plaintiff and the Class.

82. Plaintiff is represented by experienced counsel who are qualified to litigate this case. The lawsuit will be capably and vigorously pursued by Plaintiff and her counsel.

83. A class action is superior to other available methods for a fair and efficient adjudication of this controversy since joinder of all members of the Class is impracticable. Furthermore, the damages suffered by individual class members may be relatively small in comparison with the expense and burden associated with individual litigation, which make it impossible for them to individually redress the harm done to them. Proceeding as a class action will permit an orderly and expeditious administration of the claims of Class members, will foster

economies of time, effort, and expense and will ensure uniformity of decision. There will be no difficulty in the management of this litigation as a class action.

COUNT I
NEGLIGENCE

84. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

85. Anthem had a duty to exercise reasonable care to protect and secure Plaintiff's and the members of the Class's personal health, identification, and financial information in its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential personal health, identification, and financial information includes but is not limited to full legal names, birth dates, Social Security numbers, medical identification numbers, health histories, street addresses, email addresses, employment information, income data, and other personal information.

86. Anthem's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the members of the Class's personal health, identification, and financial information in their possession was adequately secured and protected and was retained only for legitimate purposes and with adequate storage, retention, and disposal policies.

87. Anthem further had a duty to implement processes that would detect a breach of its security systems in a timely manner.

88. In light of the special relationship between Plaintiff and members of the Class and Anthem, whereby Anthem required Plaintiff and members of the Class to provide highly sensitive confidential personal health, identification, and financial information as a condition of

application, availability of health insurance, and employment, Anthem undertook a duty of care to ensure the security of such information.

89. Anthem also knew or should have known that hackers would target the highly confidential personal health, identification, and financial information of Plaintiff and the members of the Class. Indeed, countless data breaches in just the past year have exploited similarly lax security controls to gain access to company-wide databases. Moreover, a number of these data breaches have targeted medical companies/institutions and the personal health, identification, and financial information of their patients/customers. As a result, it was quite clear, or at least reasonably foreseeable, that the information of Plaintiff and the members of the Class was a high value target to criminal third parties. Anthem thus had a duty to take reasonable steps in protecting this information.

90. Through its acts or omissions, Anthem breached its duty to use reasonable care to protect and secure Plaintiff's and the members of the Class's personal health, identification, and financial information in its possession or control. Anthem breached its duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and members of the Class's personal health, identification and financial information, failing to adequately monitor the security of its network, allowing unauthorized access to Plaintiff's and the members of the Class's personal health, identification and financial information, and failing to recognize in a timely manner that Plaintiff's and members of the Class's personal health, identification, and financial information had been compromised.

91. Anthem's failure to comply with widespread industry standards relating to data security further evinces Anthem's negligence in failing to exercise reasonable care in

safeguarding and protecting Plaintiff's and the members of the Class's personal health, identification, and financial information in its possession or control.

92. But for Anthem's wrongful and negligent breach of the duties owed to Plaintiff and the members of the Class, the Data Breach would not have occurred and Plaintiff's and the members of the Class's personal health, identification, and financial information would not have been compromised.

93. The injury and harm suffered by Plaintiff and the members of the Class was the reasonably foreseeable and probable result of Anthem's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the members of the Class's personal health, identification, and financial information in its possession or control. Anthem knew or should have known that its systems and technologies for processing and securing Plaintiff's and members of the Class's personal health, identification, and financial information had significant vulnerabilities.

94. As a result of Anthem's negligence, Plaintiff and the members of the Class have incurred damages, including, but not limited to, the increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse.

COUNT II
BREACH OF CONTRACT

95. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

96. When Anthem required Plaintiff and the members of the Class to supply their personal health, identification and financial information, Anthem entered into implied contracts with Plaintiff and the members of the Class to protect the security of such information.

97. Such implied contracts arose from the course of conduct between Plaintiff and the members of the Class and Anthem.

98. The implied contracts required Anthem to safeguard and protect Plaintiff's and the members of the Class's personal health, identification, and financial information from being accessed, compromised, and/or stolen.

99. Anthem did not safeguard or protect Plaintiff's and the Class members' personal health, identification, and financial information from being accessed, compromised, and/or stolen. Anthem did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and the Class members' personal health, identification and financial information.

100. Because Anthem failed to safeguard and/or protect Plaintiff's and the Class members' personal health, identification, and financial information from being accessed, compromised or stolen, Defendant breached its contracts with Plaintiff and the members of the Class.

101. Plaintiff and the members of the Class have suffered and will continue to suffer damages as the result of Anthem's breach.

COUNT III
NEGLIGENCE *PER SE*

102. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

103. HIPAA was designed to protect the privacy of personal medical information by limiting its disclosure.

104. HIPAA seeks to protect the privacy of protected patient personal health, identification, and financial information by prohibiting any voluntary or involuntary use or

disclosure of such data in violation of the directives set out in the statute and its regulations.

105. It is common practice for Pennsylvania and Indiana health care providers, as well as health care providers nationwide, to follow the procedures required under HIPAA in rendering services to their patients.

106. As described above, Defendant violated HIPAA by failing to maintain the confidentiality of its protected patient personal health, identification and financial information.

107. Plaintiff and the proposed Class members have suffered harm, including but not limited to expenses for credit monitoring, loss of privacy, and other economic and non-economic harm, as well as an being placed at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse as a result of Defendant's violation.

108. Plaintiff and the proposed Class members are persons whom Congress intended to be protected by HIPAA.

109. Defendant is a HIPAA-covered entity.

110. The personal health, identification, and financial information of Plaintiff and the Class members are the types of records HIPAA was created to protect.

111. The injuries suffered by Plaintiff and the proposed Class members were directly and proximately caused by Defendant's violation of HIPAA.

112. Defendant's violation of HIPAA thus constitutes negligence *per se* and Plaintiff and the proposed Class members are entitled to recover damages in an amount to be proven at trial.

COUNT IV
BAILMENT

113. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

114. Plaintiff and the proposed Class members delivered their personal health, identification, and financial information to Defendant in order to receive health care services from Defendant's affiliated health care providers.

115. This personal health, identification, and financial information was furnished to Defendant for the exclusive purpose of administering and managing health care services delivered by Defendant's affiliated health care providers and Defendant took possession of the personal health, identification, and financial information for the same reason.

116. Upon delivery, Plaintiff and the proposed Class members intended and understood that Defendant would adequately safeguard their personal health, identification, and financial information and Defendant, in accepting possession, understood the expectations of Plaintiff and the proposed Class members. Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

117. Pursuant to the bailment arrangement, Defendant owed Plaintiff and the proposed Class members a duty of reasonable care in safeguarding and protecting their personal health, identification and financial information.

118. This duty was breached by Defendant's failure to take adequate steps to cure the deficiencies in its security protocols and Defendant's failure to conform to best practices and industry standards to prevent unauthorized access to Plaintiff's and the proposed Class members' personal health, identification and financial information.

119. As a direct proximate result of Defendant's breach, the personal health, identification, and financial information of Plaintiff and the proposed Class members was exposed to third parties and thereafter stolen, resulting in damage to the Plaintiff and the proposed Class members as detailed herein.

COUNT V
UNJUST ENRICHMENT

120. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

121. Plaintiff brings Count V in the alternative to his claim for breach of contract.

122. Defendant received payment from Plaintiff and the proposed Class members to perform services that included protecting Plaintiff's and the proposed Class members' personal health, identification and financial information.

123. Defendant did not protect Plaintiff's and the proposed Class members' personal health, identification and financial information, but retained Plaintiff's and the proposed Class members' payments.

124. Defendant retained the benefits of Plaintiff's and the proposed Class members' payments under circumstances which rendered it inequitable and unjust for Defendant to retain such benefits without paying for their value.

125. Defendant has knowledge of said benefits.

126. As a result, Plaintiff and the proposed Class members have been proximately harmed and/or injured as described herein.

COUNT VI
VIOLATION OF INDIANA CODE §§ 24-5-0.5, *et seq*. THE INDIANA DECEPTIVE CONSUMER SALES ACT ("IDCSA")

127. Plaintiff incorporates and re-alleges each and every allegation contained above as if fully set forth herein.

128. Defendant is a citizen of Indiana and thus Indiana law applies to all of its transactions nationwide.

129. Defendant is a "supplier" for the purposes of the IDCSA because Defendant

"regularly engages in or solicits consumer transactions." IC § 24-5-0.5-2(a)(3)(A).

130. Defendant's provision and sale of services to Plaintiff and members of the proposed Class are "consumer transactions" under the IDCSA because they are a "sale . . . of a service . . . to a person for purposes that are primarily personal, familial, charitable, agricultural, or household, or a solicitation to supply any of these things." IC § 24-5-0.5-2(a)(1).

131. Defendant's inadequate security with respect to Plaintiff's and the proposed Class members' personal financial, medical, and identification information, despite Defendant's promise to protect and safeguard such information constitutes a deceptive and unconscionable consumer sale practice in violation of the IDCSA. Anthem also failed to disclose that its data security practices were sub-standard, not in line with best practices, and far below what is considered even minimally reasonable despite the fact that it represented to Plaintiff and the proposed Class members that it would protect their highly sensitive personal information and that it had a more than adequate network in place to do so.

132. Defendant also violated the IDCSA by failing to immediately notify Plaintiff and the proposed Class members of the Data Breach. Had Plaintiff and the proposed Class members been notified in a timely and appropriate fashion, they could have taken precautions to safeguard their patient identification data.

133. Defendant specifically violated the IDCSA because Defendant represented that its provision of insurance services and sale of insurance policies "ha[d] . . . characteristics, . . . uses, or benefits it [did] not have" and Defendant knew or reasonably should have known that its services did not have the represented characteristics, uses, or benefits. IC § 24-5-0.5-3(b)(1).

134. Defendant made specific representations of fact that its provision of insurance and sale of insurance policies included the protection of confidentiality of personal information.

However, Defendant knew that this was not the case as Defendant utilized sub-standard data security during the handling and storage of the personal information of Plaintiff and the proposed Class.

135. Defendant specifically violated the IDCSA because Defendant represented that its provision of insurance services and sale of insurance policies were "of a particular standard, quality, grade, style, or model" even though the services were not of the represented standard, quality, grade, style, or model and Defendant knew or reasonably should have known the same. IC § 24-5-0.5-3(b)(2).

136. Defendant represented that its provision of insurance and sale of insurance policies were secure services/products and that administrative staff and procedures were in place to protect any information used in the provision and sale of these services/products. However, Defendant knew that this was not the case as Defendant utilized sub-standard data security during the handling and storage of the personal information of Plaintiff and the proposed Class.

137. Defendant specifically violated the IDCSA because Defendant represented "[t]hat a specific price advantage exist[ed] as to [the provision of its insurance services and sale of insurance policies]", although that price advantage did not exist and Defendant knew or reasonably should have known the same. IC § 24-5-0.5-3(b)(6).

138. The deceptive and unconscionable actions of Defendant were done in the course of business, trade, and commerce. Further, a negative impact on the public interest was caused by Defendant's conduct.

139. Plaintiff and the proposed Class have suffered damages, as a result of Defendant's unfair acts and/or deceptive practices in the form of expenses for credit monitoring, lost work time, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm,

as well as being placed at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse.

140. The actions of Defendant were taken willfully, knowingly, or in reckless disregard of the interests of consumers such as Plaintiff and the proposed Class members, thereby justifying the award of three times actual damages or one thousand dollars for each violation. IC § 24-5-0.5-4(a)(1)-(2).

PRAYER FOR RELIEF

141. Plaintiff requests that this Court enter judgment against Defendant and in favor of Plaintiff and the proposed Class members and award the following relief:

A) That this action be certified as a Class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as the representative of the Class and Plaintiff's counsel as counsel for the Class;

B) Monetary damages;

C) Injunctive relief, including but not limited to the provision of credit monitoring services for Plaintiff and the proposed Class members for a period of at least 25 years, the provision of bank monitoring services for Plaintiff and the proposed Class members for a period of at least 25 years, the provision of credit restoration services for Plaintiff and the proposed Class members for a period of at least 25 years, and the provision of identity theft insurance for Plaintiff and the proposed Class members for a period of at least 25 years;

D) Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E) Costs;

F) Pre and post judgment interest;

G) Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P 38(b), Plaintiff, individually and on behalf of the Class he seeks to represent, hereby demands a trial by jury on all causes of action asserted in this action so triable.

Dated: May 21, 2015

By: /s/ Gary F. Lynch

Gary F. Lynch
Edwin J. Kilpela, Jr.
Jamisen A. Etzel
CARLSON LYNCH SWEET & KILPELA, LLP
PNC Park
115 Federal Street, Suite 210
Pittsburgh, PA 15212
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
glynch@carlsonlynch.com
ekilpela@carlsonlynch.com
jetzel@carlsonlynch.com

Karen Hanson Riebel
Heidi M. Silton
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401-2159
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
khriebel@locklaw.com
hmsilton@locklaw.com
kmbaxter-kauf@locklaw.com

Jayne A. Goldstein
POMERANTZ LLP
1792 Bell Tower Lane, Suite 203
Weston, Florida 33326
Telephone: (954) 315-3454
Facsimile: (954) 315-3455

jagoldstein@pomlaw.com

W. Daniel "Dee" Miles, III
Larry A. Golston
Andrew E. Brashier
BEASLEY, ALLEN, CROW, METHVIN, PORTIS & MILES, P.C.
272 Commerce Street
Post Office Box 4160
Montgomery, Alabama 36103-4160
(334) 269-2343
(334) 954-7555 FAX
dee.miles@beasleyallen.com
larry.golston@beasleyallen.com
andrew.brashier@beasleyallen.com

Bryan L. Bleichner
Francis J. Rondoni
Jeffrey D. Bores
CHESTNUT CAMBRONNE PA
17 Washington Avenue North, Suite 300
Minneapolis, MN 55401
Tel: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
frondoni@chestnutcambronne.com
jbores@chestnutcambronne.com

Joseph P. Guglielmo
David R. Scott
Erin Green Comite
SCOTT & SCOTT, ATTORNEYS AT LAW
156 South Main Street
P.O. Box 192
Colchester, CT 06415
Tel.: (860) 537-5537
Fax: (860) 537-4432
jguglielmo@scott-scott.com
david.scott@scott-scott.com
ecomite@scott-scott.com